

### **REMARKS/ARGUMENTS**

The Office Action mailed August 3, 2004 has been reviewed and carefully considered. Claims 1 and 7 have been amended. Claims 1-13 are pending in this application, with claims 1 and 7 being the only independent claim. Reconsideration of the above-identified application, as herein amended and in view of the following remarks, is respectfully requested.

In the Office Action mailed August 3, 2004, claims 1-13 stand rejected under 35 U.S.C. §103 as unpatentable over U.S. Patent No. 6,418,146 (Miloslavsky) in view of U.S. Patent No. 6,463,474 (Fuh).

Before discussing the cited prior art and the Examiner's rejections of the claims in view of that art, a brief summary of the present invention is appropriate. The present invention relates to an auto login proxy incorporated into a WAP gateway which is connected between a wireless network and the Internet. The auto login proxy keeps a file in which it creates an entry containing the user's name/password pair for each server on the internet that the wireless user has logged onto (see, e.g., page 3, lines 4-6, of the specification). When the user subsequently logs onto the server, the gateway retrieves that user-name/password pair from the auto login proxy and forwards the user-name/password pair to the server so that the user can log in without having to input the username/password on the wireless device (page 3, lines 6-8). The purpose of the present invention is to simplify the login procedure to network servers from wireless devices (page 2, line 21).

Independent claims 1 and 7 are amended to clarify that (1) the gateway stores login information for WAN servers that the user has previously logged onto and (2) the gateway determines whether the user has previously logged in to a particular one of the WAN servers which

requests login information and that stored login information is forwarded from the gateway to the WAN server if the user has previously logged into the particular WAN server.

Miloslavsky discloses an integrated communications center functionality for WAP devices. The device referred to as WAP-SP 23 in Miloslavsky is a WAP enable proxy server that functions as an interface for wireless users accessing the Internet (see col. 5, lines 51-55 and col. 7, lines 51-53). That is, the WAP-SP 23 is a gateway through which wireless users access the Internet. Accordingly, the WAP-SP 23 of Miloslavsky is analogous to the gateway recited in independent claims 1 and 7. The login procedure referred to in the Office Action at col. 11, lines 60-65 and col. 13, lines 11-15 of Miloslavsky is a login of the user to the WAP-SP 23, i.e., a login to the gateway, and not a login to a particular server on the Internet requesting login information (see also Fig. 3). While Miloslavsky discloses at col. 10, lines 4-10, and col. 13, lines 16-20, that the WAP-SP manages profile data which may be sent to a server, Miloslavsky fails to teach or suggest that the profile data includes login information for logging into the call destination server. Since Miloslavsky discloses only logging a wireless user into the WAP-SP 23, Miloslavsky fails to teach or suggest (1) determining, by the gateway, whether the user has previously logged in to one of the WAN servers and (2) forwarding the stored login information from the gateway to the WAN server if the user has previously logged into the particular WAN server, as recited in independent claims 1 and 7.

Fuh fails to disclose what Miloslavsky lacks. As explained below, Fuh discloses a firewall controlling access to an intranet, the firewall being connected to an authentication proxy for authenticating the user of a packet sent to a target server in the intranet. This authentication disclosed by Fuh does not teach or suggest (1) determining, by the gateway, whether the user has previously logged in to one of the WAN servers and (2) forwarding the stored login information

from the gateway to the WAN server if the user has previously logged into the particular WAN server, as recited in independent claims 1 and 7.

Fuh relates to authentication of a user at a firewall 210 which controls remote access to an intranet 216. In an example disclosed by Fuh, the user 302 connected to a LAN 206 requests information from a target server 222 connected to the intranet 216 (see Figs. 2-3; col. 8, lines 57-63). An authentication proxy 400 is connected to the firewall 210 (col. 10, lines 7-8). Instead of authenticating a user in the intranet 216, the authentication proxy attempts to provide a local authentication of the user at the firewall 210. The Authentication proxy 400 thus authenticates the user for the intranet and does not authenticate or authorize the user for the destination server. Once the authentication is accomplished, the firewall allows the client 306 to communicate with the target server 222 using standard HTTP request-response communications (col. 15, lines 12-15).

Since Fuh discloses determining whether a user is authenticated in the intranet in which a target server is connected, Fuh fails to disclose determining whether the particular user has previously logged into the target server, i.e., a particular server, as expressly recited in independent claims 1 and 7. Furthermore, since Fuh discloses that communications between the user and target server take place using standard HTTP request-response communications after authentication, Fuh also fails to disclose forwarding the stored login information from the gateway to the WAN server if the user has previously logged into the particular WAN server, as expressly recited in independent claims 1 and 7.

Dependent claims 2-6 and 8-16, each being dependent on one of independent claims 1 and 7, are deemed allowable for the same reasons expressed above with respect to independent claims 1 and 7.

New dependent claims 14 and 17 are added to recite that the login request is received by the gateway from the user. Support for this limitation is found on page 7, lines 4-6.

New claims 15 and 18 are added to recite that the login information in the login request from the user is compared to the stored login information, and that the new login information is stored if it is different than the stored login information. Support for this limitation is on page 7, lines 11-15.

New claims 16 and 19 are added to recite that the login request is received by the gateway as a WML page from the particular server. Support for this limitation is found on page 6, lines 9-17.

It is respectfully submitted that none of the prior art of record discloses, teaches or suggests, the additional limitations of claims 14-19.

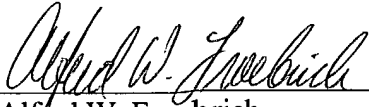
The application is now deemed to be in condition for allowance and notice to that effect is solicited.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By

  
Alfred W. Froebrich  
Reg. No. 38,887  
551 Fifth Avenue, Suite 1210  
New York, New York 10176  
(212) 687-2770

Dated: November 18, 2004